



Office of the Secretary

[Docket No. DOT-OST- 2021-0094]

Privacy Act of 1974; Department of Transportation, Federal Aviation Administration; DOT/FAA-815; Investigative Record System; System of Record Notice

**AGENCY:** Office of the Departmental Chief Information Officer, Office of the Secretary of Transportation, DOT.

**ACTION:** Notice of a Modified System of Records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the United States Department of Transportation (DOT), Federal Aviation Administration (FAA) proposes to update and reissue a current DOT system of records titled, “DOT/FAA-815, Investigative Record System.” The system collects information on FAA employees, contractors, and members of the public in support of the Personnel Security Background and Internal investigations programs. The records in this system document all official actions taken on individuals who are subject to this notice. This Privacy Act System of Records Notice (SORN) is being updated to include substantial changes to system location, system manager, authority for maintenance, purpose, categories of individuals, categories of records, records source category, routine uses, practices for storage of records, policies and practices for retrieval of records, policies and practices for retention and disposal of records, and exemptions claimed and non-substantial changes to administrative, technical and physical safeguards, records access, contesting records, and notification procedures.

**DATES:** Written comments should be submitted on or before [\*\*\[INSERT DATE 30 DAYS FROM PUBLICATION DATE IN THE FEDERAL REGISTER\]\*\*](#) The Department may publish an amended SORN in light of any comments received. This new system will be effective [\*\*\[INSERT DATE 30 DAYS FROM PUBLICATION DATE IN THE FEDERAL REGISTER\]\*\*](#).

**ADDRESSES:** You may submit comments, identified by docket number DOT-OST- 2021-0094 by any of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *Mail:* Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Ave. SE., West Building Ground Floor, Room W12–140, Washington, DC 20590–0001.
- *Hand Delivery or Courier:* West Building Ground Floor, Room W12–140, 1200 New Jersey Ave. SE., between 9 a.m. and 5 p.m. ET, Monday through Friday, except Federal Holidays.
- *Fax:* (202) 493–2251.
- *Instructions:* You must include the agency name and docket number DOT-OST- 2021-0094
- All comments received will be posted without change to <https://www.regulations.gov>, including any personal information provided.

*Privacy Act:* Anyone is able to search the electronic form of all comments received in any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the DOT’s complete Privacy Act statement in the Federal Register published on April 11, 2000 (65 FR 19477–78), or you may visit <https://DocketsInfo.dot.gov>.

*Docket:* For access to the docket to read background documents or comments received, go to <https://www.regulations.gov> or to the street address listed above. Follow the online instructions for accessing the docket.

**FOR FURTHER INFORMATION CONTACT:** For questions, please contact: Karyn Gorman, Acting Departmental Chief Privacy Officer, Privacy Office, Department of Transportation, Washington, D.C. 20590; [privacy@dot.gov](mailto:privacy@dot.gov); or (202) 527-3284.

## **SUPPLEMENTARY INFORMATION:**

### **I. Background**

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Transportation (DOT), Federal Aviation Administration (FAA) proposes to update and reissue a DOT system of records titled, “DOT/FAA 815 Investigative Records System”. The FAA requires personnel security

background investigations for current and potential FAA employees (inclusive of FAA federal government employees, interns, employees from other federal agencies on a detail, contractors and persons performing business), for suitability for federal government employment within the FAA. The investigations include decisions regarding the suitability of a security clearance and issuance of a Personal Identity Verification (PIV) card for physical and logical access to FAA controlled facilities and information systems. In addition, the FAA conducts internal investigations to include suspected criminal and civil violations by FAA employees and contractors, aircraft owners, and airmen and other FAA certificate holders as defined by 49 United States Code (USC) § 40102(a)(8), including an individual: (1) in command, or as pilot, mechanic, or member of the crew, who navigates aircraft when under way; (2) who is directly in charge of inspecting, maintaining, overhauling, or repairing aircraft, aircraft engines, propellers, or appliances (except to the extent the FAA Administrator may provide otherwise for individuals employed outside the United States); or (3) who serves as an aircraft dispatcher or air traffic control tower operator. Internal investigations may include, but are not limited to, counterfeit certificates; falsification of official documents; property theft; laser incidents; and other investigative services provided to law enforcement agencies. The system of records supports the FAA's mandate to investigate the actual or probable violation of civil and criminal laws regulating controlled substances by aircraft owners and airmen. The FAA conducts Personnel Security Background and Internal investigation services to the FAA and aviation communities to ensure aviation safety, support national security, and promote an efficient airspace system. The Investigative Records System serves as a repository of and documents the results and actions of Personnel Security Background investigations, conducted both before and after an employee's entry on duty, and internal investigations of alleged criminal and civil violations by the employees. The purpose of this system is to collect and maintain records regarding: (1) Security clearance suitability determination for pre-employment and continuous evaluation; and the issuance of a personal identity verification (PIV) card for physical and logical access to FAA controlled facilities and information systems; (2) Internal investigative records concerning employees suspected of misconduct; airmen and other FAA certificate holders suspected

of criminal activity as defined by 49 USC § 40102(a)(8); and (3) List of individuals that represent a security concern and are temporarily or permanently denied access to FAA facilities. The following substantive changes have been made to the Notice:

1. System Location: The system of records is no longer maintained by the Office of the Associate Administrator for Civil Aviation Security in Washington, D.C. The update reflects that the current system locations where hard copy records are maintained are FAA Headquarters and regional Office of Security and Hazardous Materials Safety (ASH) Offices.
2. System Manager: The system manager is updated to reflect the organizational name change of the Civil Aviation Security Office to ASH and add contact information for the system manager.
3. Authority for Maintenance of the System: The authorities are updated to include Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard 201: Policy for a Common Identification Standard for Federal Employees and Contractors, and Executive Order 13764. These authorities establish the requirements for federal agencies to conduct initial and ongoing background suitability investigations of individuals seeking employment with or access to federal facilities and information systems. Investigations have been conducted under these authorities and they are consistent with the purposes of the published SORN.
4. Purpose: The purpose section is updated to provide clarity that the system of records includes the results and actions of Personnel Security Background and Internal investigations.
5. Categories of Individuals: The categories of individuals section is updated to remove individuals involved in tort claims against the FAA because these individuals are not subjects of Personnel Security Background and Internal investigations. Additionally, the Notice breaks out and identifies the individuals subject to Personnel Background Security and Internal investigations.

6. Categories of Records: The categories of records maintained in the system section is updated to provide transparency and clarifies that the records maintained in the system of records includes, but are not limited to, Standard Form (SF)-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Positions, and SF-86 Questionnaire for National Security Positions, Office of Personnel Management (OPM) investigation results, resumes, reports from interviews and other inquiries, results of investigations and inquiries, suitability records, financial records, credit reports, medical records, educational institution records, employment records, divorce decrees, criminal records, citizenship status, and violations. These records include the following data about individuals such as name, address, date of birth, place of birth, email address, phone number, case number, alien registration number, airmen certificate number, social security number (SSN), passport number, driver's license number, biometrics, photographs, fingerprints, license plate number, vehicle identification number, bank account number and credit card number. Additionally, records about FAA employees and contractors may include FAA line of business, processing region, position, duty city and state, and contract number.

7. Records Source: The records source section is updated to include that information maintained in this system of record is collected from current and former employees, contractors, applicants, detailees, and consultants through in-person interviews, investigative reports from other Federal government agencies, state/local governments, law enforcement agencies, medical providers, credit bureaus, educational institutions, instructors, coworkers, neighbors, family members, and acquaintances.

8. Routine Uses: The previously published routine use allowing the disclosure of records pursuant to a law enforcement investigation or inquiry was duplicative of the disclosures permitted under b(7) of the Privacy Act and has been removed. In addition, this update clarifies that FAA provides the authorized representatives of United States air carriers the results of investigation of individuals that contain information related to aviation safety. Finally,

the updated Notice explicitly includes DOT Departmental General Routine Uses, previously incorporated by reference, to the extent they are compatible with the purposes of this System.

9. Records Storage: The policies and practices for the storage of records section is updated to reflect records previously stored in approved security file cabinets and containers, in file folders, on lists and forms, and in computer-processable storage media are now stored both electronically and in paper copy in a secure area accessed by authorized personnel only with a need to know.

10. Records Retrieval: The retrieval of records is updated to explicitly list all identifiers routinely used to retrieve records including date of birth, SSN, and other unique identifiers such as, case number, airmen certificate number, passport number, and alien registration number. The FAA does not retrieve records in this system of records by symbol and references to such have been removed.

11. Retention and Disposal: The retention and disposal policy is updated to include all National Archives and Records Administration (NARA) disposition schedules that are applicable to the records maintained in the system. The FAA is in the process of updating the NARA Records Control Schedule NC1-237-77-03 Investigative Case Files, December 22, 1977, to meet current business practices; however, the FAA will continue to follow current retention schedules that apply to the records that are stored in the system as follows: Item 8, Investigations to locate employee or airmen and airmen and aircraft searches, destroy records upon completion of administrative action or 5 years from date of last entry, whichever is sooner. Other investigative files should be destroyed 5 years following last completed action of litigation or 5 years from the date of last inquiry or entry into the file. Investigative correspondence files should be destroyed 3 years from date of origin. Reports about stolen aircraft and aircraft engaged in illegal activities should be destroyed 5 years after creation. Personnel security investigative reports are maintained in accordance with NARA General Records Schedule (GRS) 5.6, Security Records, item 170 and are destroyed 5 years after

separation. The copy of the OPM investigation report is destroyed when no longer needed for agency business use or upon employee separation.

Personnel security and access clearance records are maintained in accordance with NARA GRS 5.6, items 180 and 181, Personnel Security and Access Clearance Records. Per GRS 5.6, item 180, records of individuals not issued clearances are destroyed 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use. Per GRS 5.6, item 181, records of people issued clearances are destroyed 5 years after the employee or contractor relationship ends, but longer retention is authorized if required for business use. Per GRS 5.6, Item 190, Index to the Personnel Security Case Files, records are destroyed when superseded or obsolete. Per GRS 5.6, item 200, Information Security Violation Records, files should be destroyed 5 years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use.

12. Exemptions: The exemptions claimed for this system are updated to reflect the removal of Privacy Act exemption (j)(2) as the FAA is no longer a law enforcement agency as defined by the Act. The Aviation and Transportation Security Act (ATSA) (Pub. L. 107–71) transferred the principal function of civil aviation security from the FAA to the Transportation Security Administration on February 22, 2002. Legacy records created prior to the effective date of the ATSA will be afforded coverage until they have reached the appropriate disposal period. Additionally (k)(7) is listed in the Department’s Part 10 rulemaking and was not included in the previously published SORN. The Department has determined that the inclusion of (k)(7) in the regulation was done in error and will issue updated rulemaking to remove it. The Department has not exercised this exemption for this system of records. The Notice is being updated to explicitly identify the exemptions claimed for this system of records consistent with the previously published rulemaking. The system claims the following exemptions: 5 U.S.C. 552a (k)(1), (k)(2) and (k)(5). This is not a substantive change because the rulemaking was already published.

Additionally, this notice includes the following non-substantive changes to simplify and clarify the language, formatting, and text of the previously published Notice to align with the requirements of the Office of Management and Budget Memoranda A–108, and for consistency with other departmental system of records notices.

13. Administrative, Technical and Physical Safeguards: The safeguards discussion has been updated to include additional controls used to protect records, including the mandatory use of DOT/FAA issued PIV cards to access records and the capture of audit logs of all user activities.

14. The records access procedures is updated to include system manager’s contact information which is available at [https://www.faa.gov/about/office\\_org/headquarters\\_offices/ash/contacts/](https://www.faa.gov/about/office_org/headquarters_offices/ash/contacts/) for individuals seeking access to their records in the system.

15. Records Access: The contesting records and notification procedures is updated to refer the reader to the record access procedures section.

## II. Privacy Act

The Privacy Act (5 U.S.C. 552a) governs the means by which the Federal Government collects, maintains, and uses personally identifiable information (PII) in a system of records. A “system of records” is a group of any records under the control of a Federal agency from which information about individuals is retrieved by name or other personal identifier. The Privacy Act requires each agency to publish in the **Federal Register** a SORN identifying and describing each system of records the agency maintains, including the purposes for which the agency uses PII in the system, the routine uses for which the agency discloses such information outside the agency, and how individuals to whom a Privacy Act record pertains can exercise their rights under the Privacy Act (e.g., to determine if the system contains information about them and to contest inaccurate information). In accordance with 5 U.S.C. 552a(r), DOT has provided a report of this system of records to the Office of Management and Budget and to Congress.

**SYSTEM NAME AND NUMBER:** DOT/FAA – 815; Investigative Record System

**SECURITY CLASSIFICATION:** Unclassified, sensitive.



**SYSTEM LOCATION:**

Mike Monroney Aeronautical Center (MMAC), 6500 South MacArthur Boulevard, Oklahoma City, OK 73169-6901 and Office of Security and Hazardous Materials Safety (ASH), 800 Independence Avenue SW, Washington DC 20591. Hard copy records are located within ASH and locally at ASH Offices throughout the region. For a full list of ASH offices see the ASH “contact us” page on the FAA’s public facing website -

[https://www.faa.gov/about/office\\_org/headquarters\\_offices/ash/contacts/](https://www.faa.gov/about/office_org/headquarters_offices/ash/contacts/).

**SYSTEM MANAGER:**

Associate Administrator for Security and Hazardous Materials Safety, Federal Aviation Administration, 800 Independence Avenue, SW., Washington, DC 20591. Contact information is 202-267-7211.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

- Executive Order (E.O.) 13764, Amending Civil Service Rules for Security Clearances
- E.O. 12968, Access to Classified Information.
- E.O. 12829, National Industrial Security Program.
- 49 U.S.C. 44703, enacted as Subtitle E of Pub. L 100-690.
- Transportation Safety Act of 1974 (Pub. L. 93-633, Jan. 3, 1975, 88 Stat. 2156).
- 49 U.S.C. chapter 449, Air Transportation Security, enacted as Pub. L. 103–272.
- Homeland Security Presidential Directive 12 (HSPD-12).
- Federal Information Processing Standard 201: Policy for a Common Identification Standard for Federal Employees and Contractors.

**PURPOSE(S) OF THE SYSTEM:**

The Investigative Records System serves as a repository of and documents the results and actions of personnel security background investigations of pre and ongoing employment and internal

investigations of alleged criminal and civil violations. The purpose of this system is to collect and maintain records regarding:

- (1) Security clearance suitability determinations for pre-employment and continuous evaluation; and the issuance of a personal identity verification (PIV) card for physical and logical access to FAA controlled facilities and information systems;
- (2) Internal investigative records concerning employees suspected of misconduct; airmen suspected of criminal activity and other FAA certificate holders as defined by 49 USC 40102(a)(8); and
- (3) Individuals that represent a security concern and are temporarily or permanently denied access to FAA facilities.

#### **CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Personnel Security Background investigations: current and former employees, contractor and subcontractor personnel, applicants of potential employment, interns, employees from other federal agencies on detail, persons and entities performing business with FAA to include consultants, volunteers, and grantees, and sub-grantees, and applicants for FAA-funded programs. Internal investigations: lawful permanent residents, airmen, instructors, consultants, aircraft owners, flight instructors, airport operators, pilots, mechanics, designated FAA representatives, and other individuals certified by the FAA. Individuals that represent a security concern and are temporarily or permanently denied access to FAA facilities: Current and former FAA employees and contractors.

#### **CATEGORIES OF RECORDS IN THE SYSTEM:**

Results and supporting material for investigations and inquiries conducted by ASH. Categories of records maintained in this systems include but are not limited to SF-85 Questionnaire for Non-Sensitive Positions, SF-85P Questionnaire for Public Trust Positions, and SF-86 Questionnaire for National Security Positions, Office of Personnel Management (OPM) investigation results, resumes, reports from interviews and other inquiries, results of investigations and inquiries, suitability records, financial records, credit reports, medical records, educational institution records, employment

records, divorce decrees, criminal records, citizenship status, and violations. These records include the following data about individuals: name, address, date of birth, place of birth, email address, phone number, case number, alien registration number, airmen certificate number, SSN, passport number, driver's license number, biometrics, photographs, fingerprints, license plate number, vehicle identification number, bank account number and credit card number. Additionally, records about FAA employees and contractors may include: FAA line of business, processing region, position, duty station city and state, and contract number.

#### **RECORD SOURCE CATEGORIES:**

Information in this system is obtained from current and former employees, contractors, potential employees or applicants, detailees, consultants, investigative reports from other federal agencies, state/local government agencies, law enforcement agencies, medical providers, credit bureaus, educational institutions and instructors. Information may be obtained through in-person interviews with coworkers, neighbors, family members, and acquaintances.

#### **ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

##### **System Specific Routine Uses**

1. FAA provides to authorized representatives of United States air carriers the results of investigations of an individual that contain information related to aviation safety.

##### **Departmental Routine Uses**

1. In the event that a system of records maintained by DOT to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto.

2. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DOT decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

3. A record from this system of records may be disclosed as a routine use, to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

4a. Routine Use for Disclosure for Use in Litigation. It shall be a routine use of the records in this system of records to disclose them to the Department of Justice or other Federal agency conducting litigation when: (a) DOT, or any agency thereof, or (b) Any employee of DOT or any agency thereof, in his/her official capacity, or (c) Any employee of DOT or any agency thereof, in his/her individual capacity where the Department of Justice has agreed to represent the employee, or (d) The United States or any agency thereof, where DOT determines that litigation is likely to affect the United States, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or other Federal agency conducting the litigation is deemed by DOT to be relevant and necessary in the litigation, provided, however, that in each case, DOT determines that disclosure of the records in the litigation is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

4b. Routine Use for Agency Disclosure in Other Proceedings. It shall be a routine use of records in this system to disclose them in proceedings before any court or adjudicative or administrative body before which DOT or any agency thereof, appears, when: (a) DOT, or any agency thereof, or (b) Any employee of DOT or any agency thereof in his/her official capacity, or (c) Any employee of DOT or

any agency thereof in his/her individual capacity where DOT has agreed to represent the employee, or (d) The United States or any agency thereof, where DOT determines that the proceeding is likely to affect the United States, is a party to the proceeding or has an interest in such proceeding, and DOT determines that use of such records is relevant and necessary in the proceeding, provided, however, that in each case, DOT determines that disclosure of the records in the proceeding is a use of the information contained in the records that is compatible with the purpose for which the records were collected.

5. The information contained in this system of records will be disclosed to the Office of Management and Budget (OMB) in connection with the review of private relief legislation as set forth in OMB Circular No. A-19 at any stage of the legislative coordination and clearance process as set forth in that Circular.

6. Disclosure may be made to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual. In such cases, however, the Congressional office does not have greater rights to records than the individual. Thus, the disclosure may be withheld from delivery to the individual where the file contains investigative or actual information or other materials, which are being used, or are expected to be used, to support prosecution or fines against the individual for violations of a statute, or of regulations of the Department based on statutory authority. No such limitations apply to records requested for Congressional oversight or legislative purposes; release is authorized under 49 CFR Section 10.35(a)(9).

7. One or more records from a system of records may be disclosed routinely to the National Archives and Records Administration in records management inspections being conducted under the authority of 44 USC Sections 2904 and 2906.

8. DOT may make available to another agency or instrumentality of any government jurisdiction, including State and local governments, listings of names from any system of records in DOT for use in law enforcement activities, either civil or criminal, or to expose fraudulent claims, regardless of the

stated purpose for the collection of the information in the system of records. These enforcement activities are generally referred to as matching programs because two lists of names are checked for match using automated assistance. This routine use is advisory in nature and does not offer unrestricted access to systems of records for such law enforcement and related antifraud activities. Each request will be considered on the basis of its purpose, merits, cost effectiveness and alternatives using Instructions on reporting computer matching programs to the Office of Management and Budget, OMB, Congress and the public, published by the Director, OMB, dated September 20, 1989.

9. It shall be a routine use of the information in any DOT system of records to provide to the Attorney General of the United States, or his/her designee, information indicating that a person meets any of the disqualifications for receipt, possession, shipment, or transport of a firearm under the Brady Handgun Violence Prevention Act. In case of a dispute concerning the validity of the information provided by DOT to the Attorney General, or his/her designee, it shall be a routine use of the information in any DOT system of records to make any disclosures of such information to the National Background Information Check System, established by the Brady Handgun Violence Prevention Act, as may be necessary to resolve such dispute.

10. DOT may disclose records from this system, as a routine use to appropriate agencies, entities and persons when (a) DOT suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) DOT has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DOT or another agency or entity) that rely upon the, compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DOT's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

11. DOT may disclose records from this system, as a routine use, to the Office of Government Information Services for the purpose of (a) resolving disputes between Freedom of Information Act

requesters and Federal agencies and (b) reviewing agencies' policies, procedures, and compliance in order to recommend policy changes to Congress and the President.

12. DOT may disclose records from this system, as a routine use, to contractors and their agents, experts, consultants, and others performing or working on a contract, service, cooperative agreement, or other assignment for DOT, when necessary to accomplish an agency function related to this system of records.

13. DOT may disclose records from this system, to an agency, organization, or individual for the purpose of performing audit or oversight operations related to this system of records, but only such records as are necessary and relevant to the audit or oversight activity. This routine use does not apply to intra-agency sharing authorized under Section (b)(1), of the Privacy Act.

14. DOT may disclose from this system, as a routine use, records consisting of, or relating to, terrorism information (6 U.S.C. Section 485(a)(5)), homeland security information (6 U.S.C., Section 482(f)(1)), or Law enforcement information (Guideline 2 Report attached to White House Memorandum, "Information Sharing Environment, November 22, 2006) to a Federal, State, local, tribal, territorial, foreign government and/or multinational agency, either in response to its request or upon the initiative of the Component, for purposes of sharing such information as is necessary and relevant for the agencies to detect, prevent, disrupt, preempt, and mitigate the effects of terrorist activities against the territory, people, and interests of the United States of America, as contemplated by the Intelligence Reform and Terrorism Prevention Act of 2004, (Pub. L. 108-458) and Executive Order, 13388 (October 25, 2005).

#### **POLICIES AND PRACTICES FOR STORAGE OR RECORDS:**

Records in this system are stored electronically or in paper copy in a secure area accessed by authorized personnel with a need to know.

#### **POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:**

Records may be retrieved by name, date of birth, SSN, and other unique identifiers such as case number, airmen certificate number, passport number, and alien registration number.

## **POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

The FAA is in the process of updating the NARA Records Control Schedule NC1-237-77-03

Investigative Case Files, December 22, 1977, to meet current business practices; however, the FAA to will continue to follow current retention schedules that apply to the records that are stored in the system as follows: Item 8, Investigations to locate employee or airmen and airmen and aircraft searches are destroyed upon completion of administrative action or 5 years from date of last entry, whichever is sooner. Other investigations are destroyed 5 years following last completed action of litigation or 5 years from the date of last inquiry or entry into the file. Investigative correspondence files are destroyed 3 years from date of origin. Reports about stolen aircraft and aircraft engaged in illegal activities are destroyed 5 years after creation. Personnel security investigative reports are maintained in accordance with NARA General Records Schedule (GRS) 5.6, Security Records, item 170, and are destroyed 5 years after separation. The copy of the OPM investigation report is destroyed when no longer needed for agency business use or upon employee separation.

Personnel security and access clearance records are maintained in accordance with NARA GRS 5.6 items 180 and 181. GRS 5.6, Item 180, Records of people not issued clearances, are destroyed 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use. GRS 5.6, item 181, Records of people issued clearances, are destroyed 5 years after employee or contractor relationship ends but longer retention is authorized if required for business use. NARA GRS 5.6, item 190, Index to the personnel security case files, are destroyed when superseded or obsolete. NARA GRS 5.6, item 200, Information Security Violation Records are destroyed 5 years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use.

## **ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS:**

Safeguards for the records within this notice are in accordance with FAA rules and policies, to include all applicable DOT automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the



computer system containing the records in this system is limited to individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. Authorized users must use DOT/FAA issued PIV cards to access records, and all user activities on the system is captured in audit logs.

#### **RECORD ACCESS PROCEDURES:**

Individuals seeking notification of whether this system of records contains information about them may contact the System Manager at

[https://www.faa.gov/about/office\\_org/headquarters\\_offices/ash/contacts/](https://www.faa.gov/about/office_org/headquarters_offices/ash/contacts/). When seeking records about yourself from this system of records or any other Departmental system of records your request must conform to the Privacy Act regulations set forth in 49 CFR part 10. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

#### **CONTESTING RECORD PROCEDURES:**

See “Records Access Procedures” above.

#### **NOTIFICATION PROCEDURE:**

See “Records Access Procedures” above.

#### **EXEMPTIONS PROMULGATED FOR THE SYSTEM:**

This system of records is exempted from certain provisions of the Privacy Act. The purpose of the exemptions is to protect investigatory materials compiled for non-criminal law enforcement purposes. The exemptions claimed for this system are pursuant to 5 U.S.C. 552a (k)(1), (k)(2) and (k)(5).

#### **HISTORY:**

A full notice of this system of records, DOT/FAA 815, Investigative Tracking System, was published in the Federal Register on April 11, 2000 (65 FR 19520).

**Issued in Washington, DC.**

Karyn Gorman,

Acting Departmental Chief Privacy Officer.

[FR Doc. 2022-17943 Filed: 8/19/2022 8:45 am; Publication Date: 8/22/2022]